Driescher Energie-Forum

Manuel ‚HonkHase‘ Atug

Resilienz für KRITIS
im Cyberspace und physischen Schutz

Manuel ‚HonkHase‘ Atug

Manuel 'HonkHase' Atug

Principal bei der HiSolutions AG

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- Weit über 23 Jahren in der Informationssicherheit tätig
- Sachverständiger für das IT-SiG 2.0 im Bundestag
- Themen: KRITIS, Hackback, Ethik, Hybrid Warfare, Cyberresilienz, Bevölkerungs- und Katastrophenschutz
- Experte der European Research Executive Agency (EU REA)
- Mitgründer der AG KRITIS: ag.kritis.info

AG KRITIS

~~@HonkHase~~ @HonkHase@chaos.social

@honkhase.bsky.social

Ich habe #KRITIS im Endstadium

©left BlaBlaSecurity 2025 | @HonkHase

Wie ist Cybersicherheit in Deutschland organisiert?

©left BlaBlaSecurity 2025 | @HonkHase

Europäische Kommission

Your Europe
European Union

Single Digital Gateway: Einheitliches digitales Zugangstor zu den Verwaltungsleistungen der EU und der Mitgliedstaaten

EU-Mitgliedsstaaten

EU-Fristen einhalten. EU-Anforderungen mitdenken. EU-Komponenten nachnutzen.

Funktioniert das?

Bundeskanzleramt

Bundeskanzlerin
Chef des Bundeskanzleramtes
Staatsministerin für Digitalisierung

Gruppe Digitalpolitik, IT-Steuerung

Beide Projekte perspektivisch verbinden.

Digital Service 4Germany

dit.bund
DIT ist Innovation

Bundesministerium des Innern, für Bau und Heimat

Der Beauftragte der Bundesregierung für Informationstechnik

Bundesinnenminister
CIO der Bundesregierung

Abteilung Digitale Gesellschaft

Reicht der politische Wille?

BKAmt und BMI verantworten und koordinieren Umsetzung.

Monitoring auf solide Grundlage stellen! Orientierung geben!

Konferenz der Regierungschefinnen und Regierungschefs der Länder

Ministerpräsidenten

Chefs der Staats- und Senatskanzleien

Reicht der politische Wille?

Es braucht ein echtes politisches Controlling!

Die Bundesregierung

Digitalkabinett

Digitalrat der Bundesregierung

Vorschläge müssen umgesetzt werden.

daten ethik kommission

z.B. IMK WMK 2019

Fachministerkonferenzen

Reicht die Unterstützung?

Die Bundesregierung

IT-Konsolidierung Bund

IT-Rat

Informationstechnikzentrum Bund

ITZ Bund

Leistungs- und Unterstützungsfähigkeit muss erhöht werden.

FITKO

Zu wenig Personal!

unterstützen konzeptionell und operativ

KoSIT

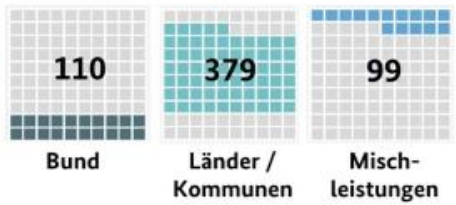
IT-Planungsrat

Bundes-CIO + Landes-CIOs
Kommunale Spitzenverbände

Zielsetzungen bis 2022

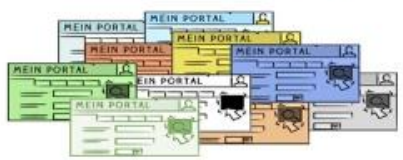
bis **2023**: Umsetzung **Single-Digital-Gateway-VO** (= EU-OZG)

1. Umsetzung der 588 **OZG-Leistungen**



2. Verknüpfung der Portale aller Ebenen zu einem **Portalverbund** (inkl. Servicekonten)

bund.de BETA
Verwaltung digital



Bundesministerien

AA | BK | BMAS
BMBF | BMEL | BMF
BMFSFJ | BMG | BMI
BMJV | BMU | BMVI
BMVG | BMWi | BMZ

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzfragen zu Registern und Datencockpit klären.

Datenschutzfragen zu Registern und Datencockpit klären.

DSK Landes-Datenschützer

IT-Dienstleister der Länder & Kommunen

IT-Unternehmen, Start-Ups

Länder und Kommunen

294 Landkreise, ca. 11.000 Gemeinden

Deutscher Städtetag | DStGB | Deutscher Landkreistag

Prinzipien

Digital First
(digitale Verfahren als Regelfall)

Once Only
(Daten nur noch einmal angeben)

Transparenz verbessern!

Bund, Länder und Kommunen entwickeln gemeinsam Lösungen.

Privates IT-Know-How besser einbinden! FIT-Store-Konzept anpassen.

Bund gibt zusätzlich 3 Mrd. Euro!

Flächendeckung fraglich! Es bleiben nur noch 2 Jahre Zeit!

Sind alle nötigen Mittel eingeplant (**1,5 Mrd. Euro**)?

Creative Commons 4.0 Namensnennung
Monitor Digitale Verwaltung #4, 09/2020
Nationaler Normenkontrollrat (NKR)

©left BlaBlaSecurity 2025 | @HonkHase

KRITIS Sektor Staat und Verwaltung digital handlungsfähig?

©left BlaBlaSecurity 2025 | @HonkHase

Die staatliche Cybersicherheitsarchitektur Deutschlands ➔

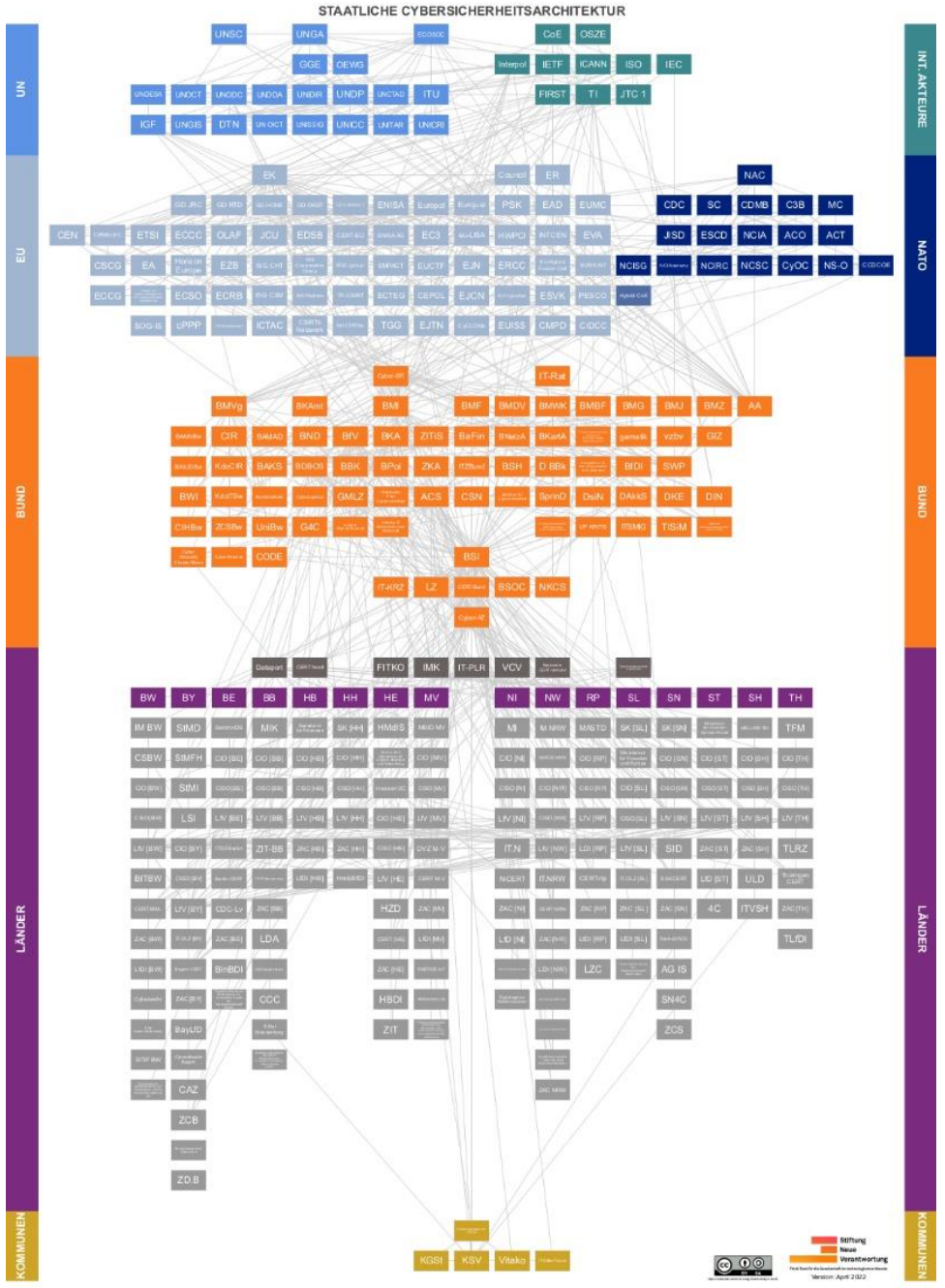
UN

Europe

Germany

Federal States

Municipalities



Int. Actors

NATO

Germany

Federal States

Municipalities

©left BlaBlaSecurity 2025 | @HonkHase

Gesetzeskarte für das Energie-versorgungs-system

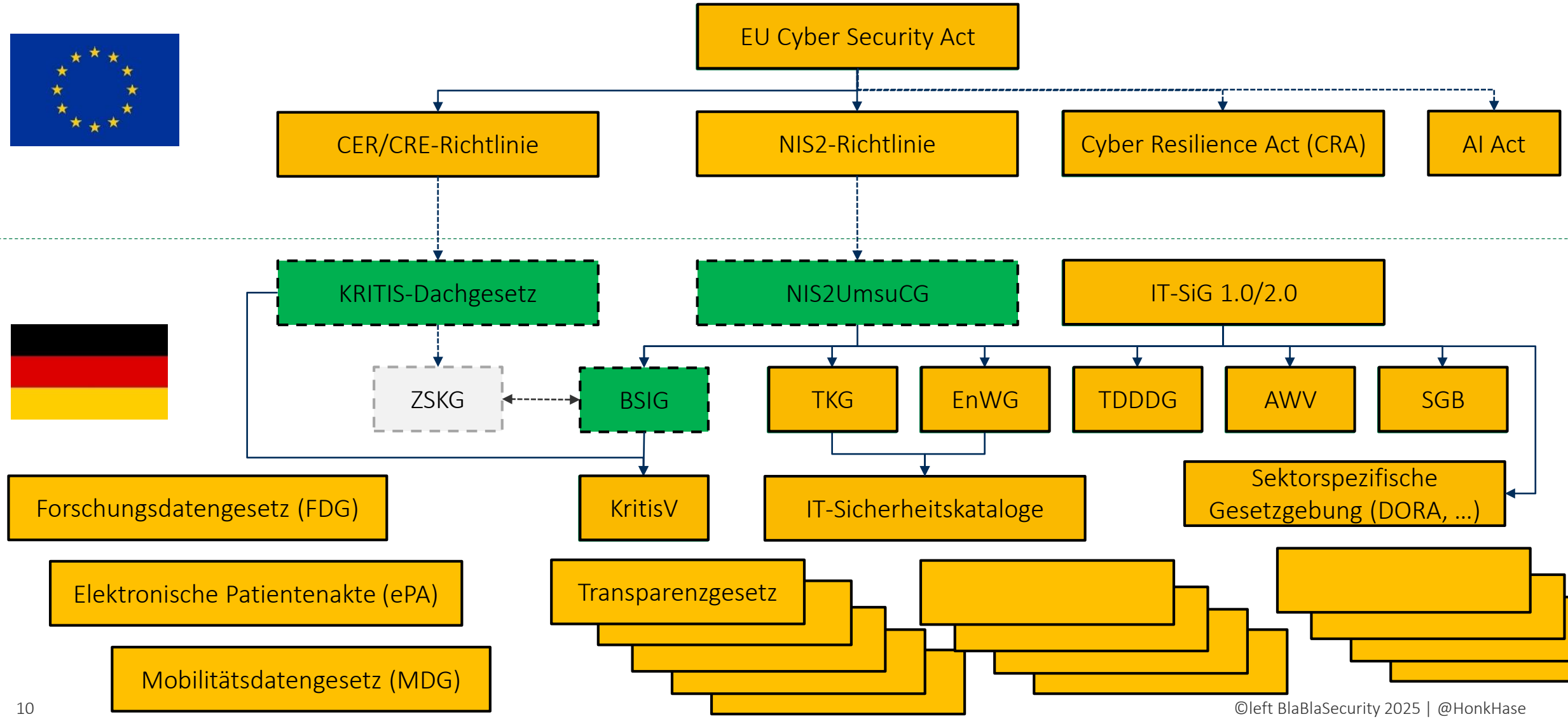
(Karte zentraler Strategien, Gesetze und Verordnungen)

©left BlaBlaSecurity 2025 | @HonkHase

Cybersicherheits- & physische Gesetzgebungen

Übersicht zur Cybersicherheitsgesetzgebung

(naja, so ein bischen halt)



©left BlaBlaSecurity 2025 | @HonkHase

NIS-2: Cybersicherheit durch Risikomanagement

Umsetzung von **angemessenen** und **verhältnismäßigen** Maßnahmen in verschiedenen Themenbereichen

Kriterien

- Risikoexposition
- Größe der Einrichtung
- Umsetzungskosten
- Eintrittswahrscheinlichkeit
- Schwere von Sicherheitsvorfällen
- Gesellschaftliche / wirtschaftliche Auswirkungen

Themenbereiche

- Risiko Management
- Informationssicherheitsmanagement
- Asset Management
- Technische Sicherheit
- Personelle & organisatorische Sicherheit
- Notfall- & Krisen Management
- Lieferanten, Dienstleister und Dritte
- Vorfallerkennung und -bearbeitung

KRITIS: Aufwändigere Maßnahmen verhältnismäßig, wenn erforderlicher Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht

©left BlaBlaSecurity 2025 | @HonkHase

Kritis Dachgesetz: Physische Sicherheit

Zu diesen Risiken gehören insbesondere ***Unfälle****,* ***Naturkatastrophen****,* ***gesundheitliche Notlagen*** *wie etwa* ***Pandemien*** *und* ***hybride Bedrohungen*** *oder* ***andere feindliche Bedrohungen****, einschließlich* ***terroristischer Straftaten****,* ***krimineller Unterwanderung*** *und* ***Sabotage****. Auch Risiken* ***sektorübergreifender grenzüberschreitender Art*** *sind zu berücksichtigen.*

Bei der ***Risikoanalyse und der Risikobewertung*** *sollen die Erkenntnisse anderer thematisch betroffener Fachressorts (z.B. diejenigen der Sicherheitsbehörden) in die Bewertungen mit einfließen.*

©left BlaBlaSecurity 2025 | @HonkHase

Die Aufgaben

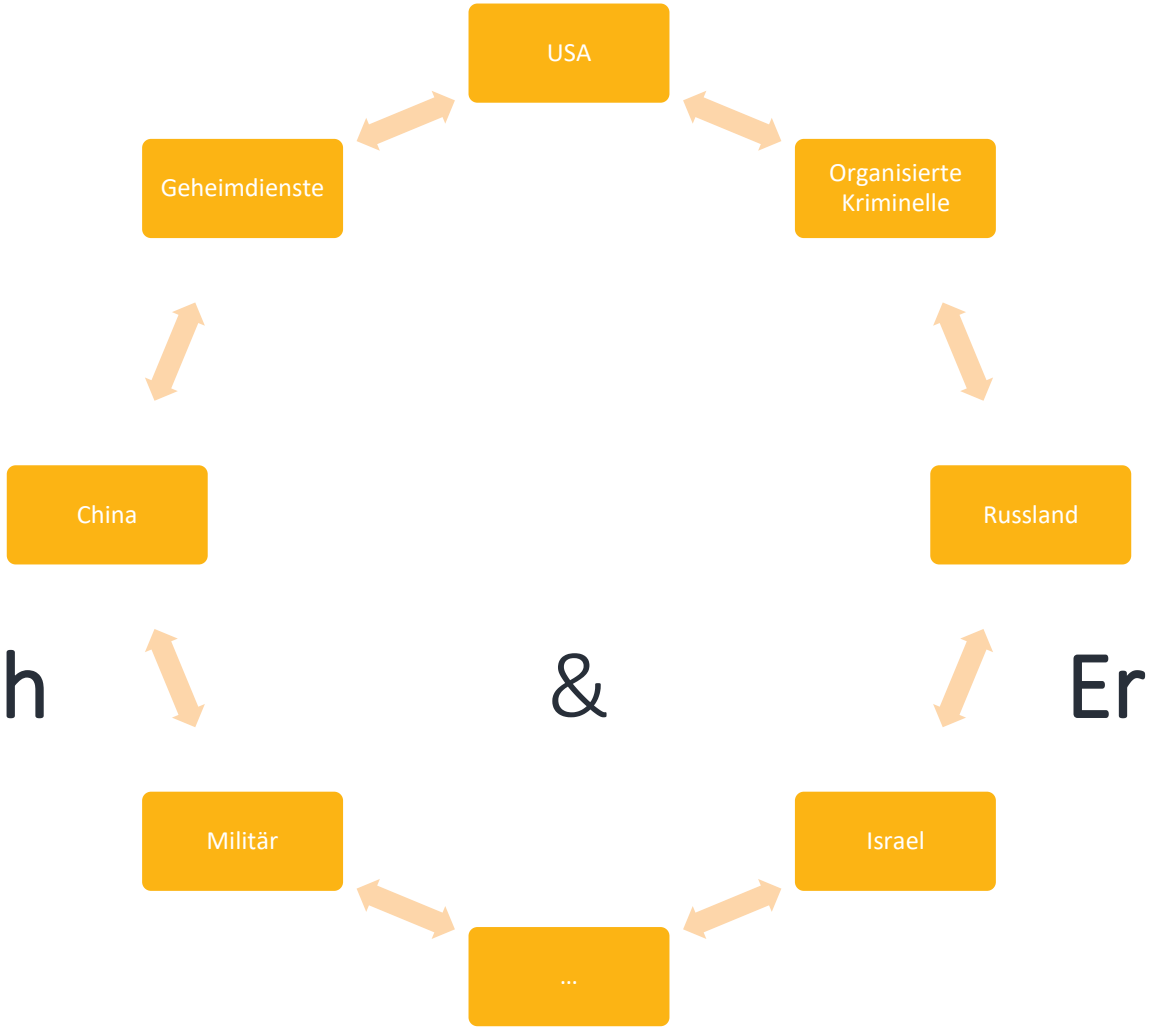
Prävention	Physischer Schutz	Vorfalls- und Krisenmanagement
Verhindern von Sicherheitsvorfällen, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel	Physischer Schutz von Räumlichkeiten und kritischen Infrastrukturen gewährleisten zum Beispiel durch Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen	Kapazitäten zur Reaktion, Abwehr und Folgeeinschränkung bei Vorfällen, unter gebührender Berücksichtigung der Umsetzung von Risiko- und Krisenmanagementverfahren und -protokollen und vorgegebener Abläufe im Alarmfall
Wiederanlauf	**Sicherheitsmanagement**	**Sensibilisierung von Personal**
Gewährleistung von Wiederherstellung, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen	Berücksichtigung von Maßnahmen wie Festlegung von Personalkategorien, Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeitsüberprüfungen, Festlegung von Schulungsanforderungen und Qualifikationen	Personal für die unter den Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren

©left BlaBlaSecurity 2025 | @HonkHase

Organisierte Kriminalität, Geheimdienste und andere staatliche Akteure

©left BlaBlaSecurity 2025 | @HonkHase

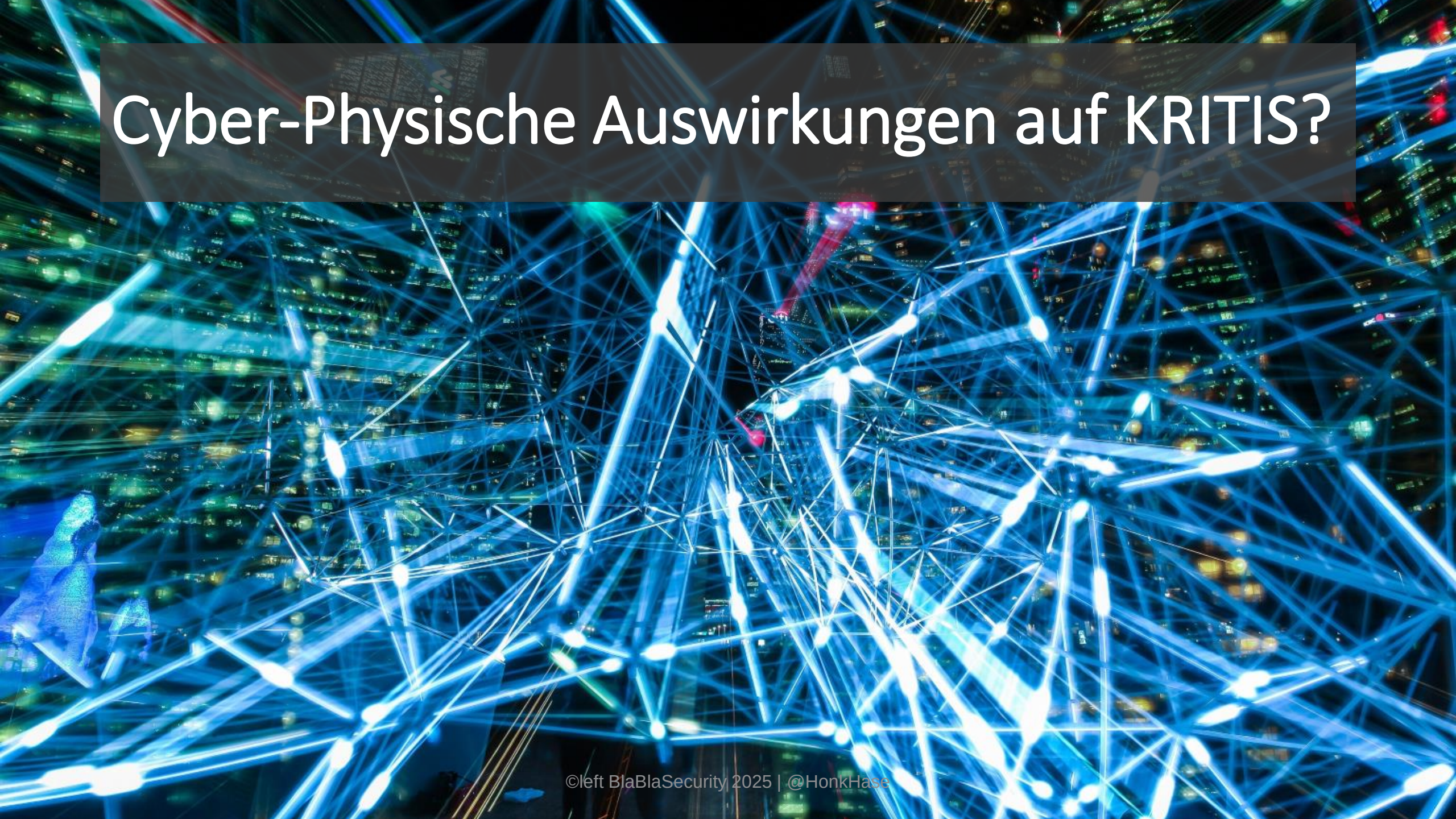
Schutz vor was und wem?



Machtmissbrauch & Erlösmaximierung

©left BlaBlaSecurity 2025 | @HonkHase

Cyber-Physische Auswirkungen auf KRITIS?

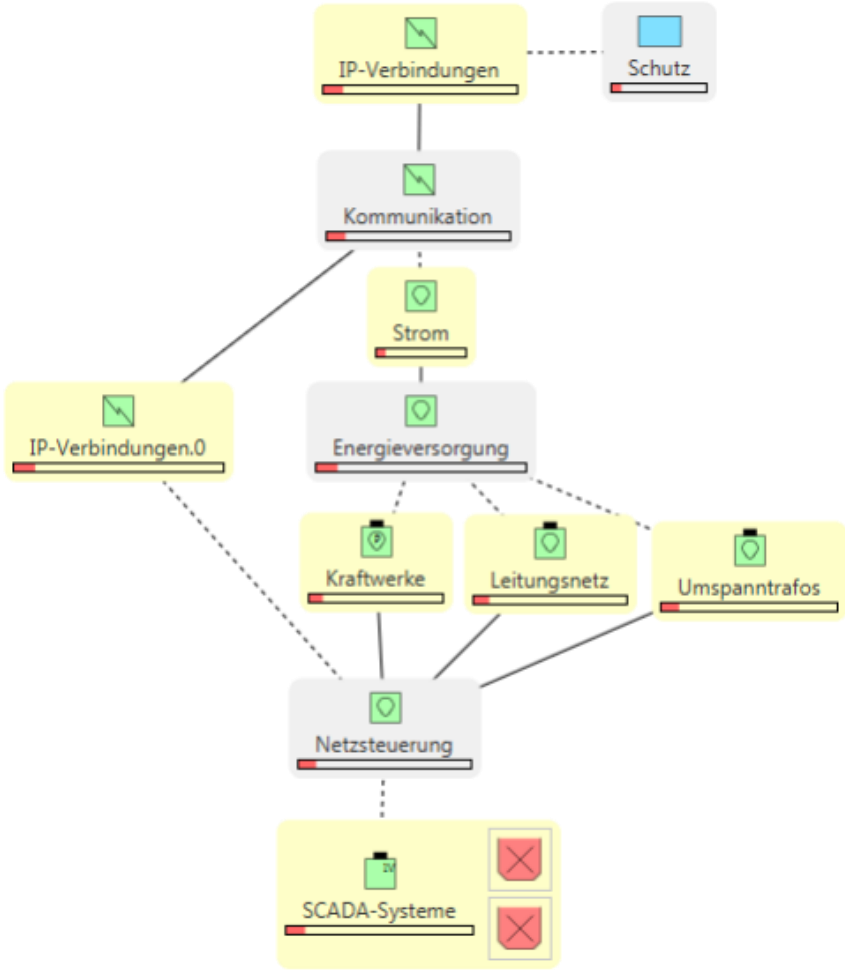


©left BlaBlaSecurity 2025 | @HonkHase

militärische Cyber-Wirkketten

(Theorie)

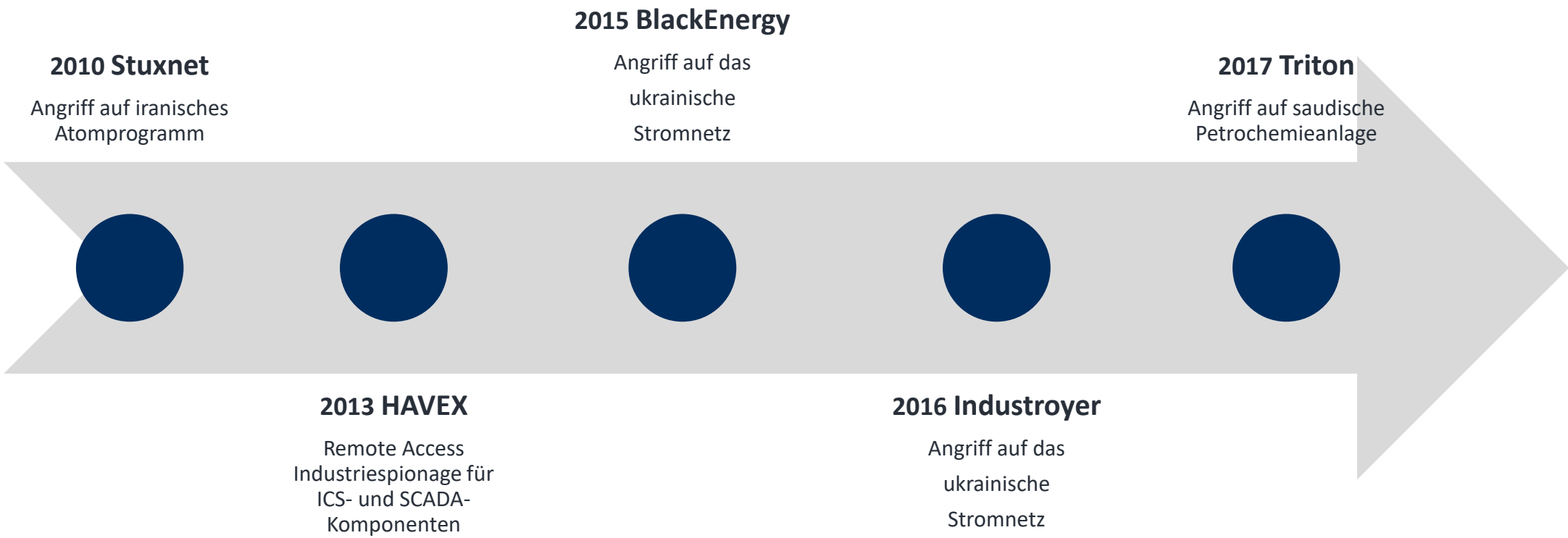
- **Cyberwirkung** löst häufig eine Kettenreaktion auf dem **Fähigkeits-Ressourcen-Netzwerk** aus
  - Angriff auf **SCADA-System** führt zum Ausfall der **Stromversorgung**
  - Ausfall der **Stromversorgung** führt zum Ausfall der **Telekommunikation**
  - Ausfall der **Telekommunikation** führt zum Ausfall/Einschränkung von **Schutzfunktion**



©left BlaBlaSecurity 2025 | @HonkHase

Timeline der wesentlichen ICS Angriffe

(Und welche davon waren Cyberwar?)



©left BlaBlaSecurity 2025 | @HonkHase

Staatliche und nicht-staatliche Akteure im Cyberraum

Es gibt nur einen gemeinsamen Cyberraum für alle. Ja, auch im Krieg!

- Militär - und damit Cyber-Kombattanten
- Geheimdienste - könnten überall dahinter stecken
- Cybercrime – Ransomware & Co
- Kritische Infrastrukturen inkl. Staat und Verwaltung
- Wirtschaft, Wissenschaft & Forschung
- Zivilgesellschaft: Bürgerinnen; ethisch noch nicht gereifte Jugendliche; destruktive „Cyber-Hooligans“; Hackerkollektive wie Anonymous

©left BlaBlaSecurity 2025 | @HonkHase

Realitätsabgleich

(Praxis)

Ja aber wir haben doch viele Millionen Cyberangriffe am Tag!!!eins!!elf!

Portscan != Angriff
Cyberangriff != Cyberwar
Hype und Angst != Cyberrealität

2 x Stromausfall in Ukraine!

Stromausfall != Blackout

Es gibt Cyber-physische Vorfälle!

- * Stuxnet
- * Projekt Aurora

Beide keine Kriegsoperation

* Sabotage durch Geheimdienste

* Wissenschaftliches Experiment

©left BlaBlaSecurity 2025 | @HonkHase

Projekt Aurora - Cyber-physischer Proof of Concept

Ist ein alter Hut

Aurora Generator Test am Idaho National Laboratory in 2007

*“The experiment used a **computer program** to **rapidly open and close** a diesel generator's **circuit breakers** out of phase from the rest of the grid and cause it to **explode**”*

Quelle: https://en.wikipedia.org/wiki/Aurora_Generator_Test

©left BlaBlaSecurity 2025 | @HonkHase

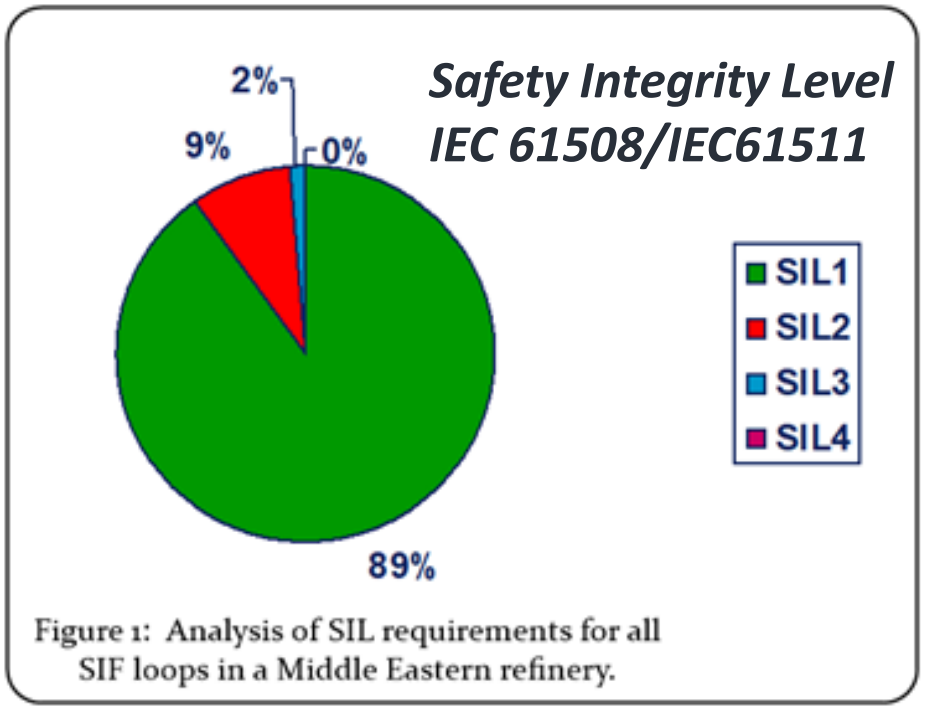


Figure 1: Analysis of SIL requirements for all SIF loops in a Middle Eastern refinery.

Triconex Tricon

Attacke auf Saudi Arabisches Petrochemiewerk

- TRITON: passiver Implant mit Remote Access Funktion
- Folge wäre gewesen: Explosionen und die Freisetzung von Schwefelwasserstoffgas

Safety-PLC gemäß Safety Instrumented System (SIL3)
Firmware wurde im RAM gezielt manipuliert

©left BlaBlaSecurity 2025 | @HonkHase

Gibt es denn Bedrohungen für KRITIS?

- Digitalisierung?
  …schreitet bei KRITIS (langsam & schlecht) voran
- Ransomware wird mehr!
- Fachkräftemangel wird mehr!
- Naturereignisse werden mehr!

- „Cyberwar-“, Geheimdienste- & Hackback Szenarien bringen zukünftig mögliche Kollateralschäden

©left BlaBlaSecurity 2025 | @HonkHase

©left BlaBlaSecurity 2025 | @HonkHase

How to Cyber: Prävention | Detektion | Reaktion

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

©left BlaBlaSecurity 2025 | @HonkHase

Cyber-Verteidigung

(it‘s all about Cyber…)

Wie? Das ist doch quasi Magie… wie KI oder Blockchain…

Cyberresilienz! Zur Erhöhung der Widerstandsfähigkeit von KRITIS

** Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen*

Warum? Angriffe verpuffen wirkungslos durch Basis-Maßnahmen

** Hallo, BSI Grundschutz*

©left BlaBlaSecurity 2025 | @HonkHase

>> All-Gefahren-Ansatz <<

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

©left BlaBlaSecurity 2025 | @HonkHase

Krisenmanagement

in 7 Schritten

Schritt 1
Wen brauche
ich im Krisenfall?

Schritt 2
Wo treffen wir uns in der Krise?

Schritt 3
Wie kommuniziere ich?

Schritt 4
Was mache ich im Krisenfall?

Schritt 5
Was brauche ich an
Dokumentation?

Schritt 6
Köpfe kennen in der Krise

Schritt 7
(Cyber-)Versicherung?

©left BlaBlaSecurity 2025 | @HonkHase

How to Backup

(…die langweiligen Basics der IT-Security)

- Habt ihr ein Backup erstellt?
- Ist es frisch oder fermentiert es vor sich hin?
- Habt ihr das sogar Offline vorliegen?
- Habt ihr mal die Wiederherstellung getestet?

Denkt dran:

- Cloud Speicher ist kein Backup!
- Beim KFZ fragt man auch die Werkstatt

©left BlaBlaSecurity 2025 | @HonkHase

Frage der Bevölkerung: Kommt morgen noch Strom & Wasser aus der Leitung?

©left BlaBlaSecurity 2025 | @HonkHase

Cyberresilienz ➔ Widerstandsfähigkeit gegen Ereignisse

- Ursache für Katastrophe oder Cybervorfall ist für die Bevölkerung nicht relevant

- Aber: eine Krise (Pandemie) in der Krise (Putins Angriffskrieg) in der Krise (Ransomware) in der Krise (Gasmangellage) in der ***<beliebige Krise hier einfügen>*** braucht keiner!

- Kritische Fragen:

  → Ist Digitalisierung immer erforderlich?

  →Können wir damit die Cyberresilienz erhöhen?

  →Was ist eine gute Digitalisierung?

©left BlaBlaSecurity 2025 | @HonkHase

Nachhaltigkeit in der Digitalisierung

- Bei der digitalen Transformationen verantwortungsvolle Maßnahmen einzuleiten und gewissenhaft durchzuführen, also zu operationalisieren, ist daher gleichsam eine technische wie ethische Aufgabe!
- Vermeidet daher technische Schulden an kommende Generationen
- Hinter jedem Datensatz steht ein Mensch ➔ Daten können toxisch sein
- Security by Design und Privacy by Design ist Menschenschutz

©left BlaBlaSecurity 2025 | @HonkHase

>> All-Gefahren-Ansatz <<

„Berücksichtigung aller Gefahrenarten (z. B. Naturgefahren, technologische Gefahren, etc.) im Rahmen des Risiko- und Krisenmanagements“

** Hallo BBK*

©left BlaBlaSecurity 2025 | @HonkHase

Und was mache ich, wenn alles nichts hilft?

©left BlaBlaSecurity 2025 | @HonkHase

Irgendwas mit Holz?

Kokosnusspflücker!

www.kokosnusspflücker.de

©left BlaBlaSecurity 2025 | @HonkHase